



2024 CAE Community Symposium

Red-Teaming the NCAE Cyber Games

Spencer Hall- NCAE Cyber Games Red Team Co-lead
James Rice- NCAE Cyber Games Participant Preparation Lead



**NCAE
CYBERGAMES**
PLAY | LEARN | PROTECT

2024 CAE Symposium

Where we started
(First joined the team)

```
ftp.sh 408 B
1 #!/bin/bash
2 IP="$1"
3 FILE=TPS_Report.txt
4 USER=peter
5 PASS=
6
7 wget --timeout=3 --tries=1 --user=$USER --password=$PASS ftp://$IP/$FILE
8 rc=$?
9
10 # If file was recieved, then check is good
11 if [ "$FILE" ]; then
12     rm "$FILE"
13     exit 0
14 fi
15
16 # Couldn't connect to FTP
17 if [ $rc -eq 1 ]; then
18     exit 2
19 fi
20
21 # We connected to FTP but file not found
22 exit 1
```

```
function configureMySQL {
    if ! apt list --installed | grep -q mysql-server; then
        echo "MySQL not installed!"
        exit 1
    fi
    if [[ ! -f ${CONF} ]]; then
        echo "Could not find the file ${CONF}"
        exit 1
    fi
    # mysql directive doesnt exist, add it and config line
    if ! grep -q "\[mysqld\]" "${CONF}"; then
        echo "[mysqld]" >> "${CONF}"
        echo "skip-grant-tables" >> "${CONF}"
    else
        # add our config line after mysql directive
        sed -i 's/\[mysqld\]/\[mysqld\]\nskip-grant-tables/g' "${CONF}"
    fi
}
configureMySQL
```

```
setup_grub_timer.sh 529 B
1 #!/bin/bash
2 #
3 # File: setup_grub_timer.sh
4 # Sets the grub timer to parameter passed and ensures the grub timer is
5 # not hidden. Default timer is 15
6 #
7 # Parameters:
8 # 1 - time in seconds
9 # 2 - file path to the grub config
10
11 set -e
12
13 if [[ $EUID -ne 0 ]]; then
14     echo "Run as root!"
15     exit 1
16 fi
17
18 timer="${1:-15}"
19 fpath="${2:-/etc/default/grub}"
20
21 # Replace the entire GRUB_TIMEOUT line
22 sed -i "/GRUB_TIMEOUT=/c\GRUB_TIMEOUT=${timer}" "${fpath}"
23 sed -i "/^GRUB_TIMEOUT_STYLE=/c\#GRUB_TIMEOUT_STYLE=hidden" "${fpath}"
24 update-grub
```



2024 CAE Community Symposium

Where we initially expanded

```
$ docker-compose exec -it provisioner pvs
loaded 0 YAML plugin(s) from /data/provisioner/provisioner/plugins
loaded 1 Python plugin(s) from /data/provisioner/provisioner/plugins
loaded 73 YAML plugin(s) from ../provisioner-plugins
loaded 0 Python plugin(s) from ../provisioner-plugins
[01:26:36] [default_event] provisioner > show options
Config      Value
-----
job!targets set()
job!event_id default_event

ansible!password None
ansible!user      ansible
ansible!become    True
ansible!become_user root
ansible!become_password None
ansible!become_method sudo
ansible!gather_facts True
ansible!ssh_key   ~/.ssh/ansible_key
ansible!verbosity None
ansible!hosts     ['all']

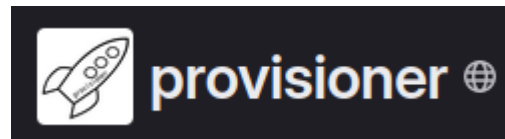
[01:26:40] [default_event] provisioner > []
```

```
[01:26:40] [default_event] provisioner > use grub_timeout
plugin now in use at: plugins.grub_timeout:0
[01:27:09] [default_event] provisioner > show options
Config      Value
-----
job!targets set()
job!event_id default_event

ansible!password None
ansible!user      ansible
ansible!become    True
ansible!become_user root
ansible!become_password None
ansible!become_method sudo
ansible!gather_facts True
ansible!ssh_key   ~/.ssh/ansible_key
ansible!verbosity None
ansible!hosts     ['all']

plugins.grub_timeout:0!grub_timeout 30
plugins.grub_timeout:0!grub_path    /etc/default/grub
plugins.grub_timeout:0!altitude    10000

[01:27:11] [default_event] provisioner > []
```



2024 CAE

Building out

```
bind_setup/tasks/main.yml 0 → 100644
1 + ---
2 + - name: Including OS Specific Variables
3 +   include_vars:
4 +     file: "{{ ansible_os_family }}.yaml"
5 +
6 + - name: Include Bind Template Variables
7 +   include_vars:
8 +     file: "Bind.yaml"
9 +
10 + - name: Install Bind Packages
11 +   package:
12 +     name: "{{ bind_packages }}"
13 +     state: present
14 +     loop: "{{ __bind_packages }}"
15 +     loop_control:
16 +       loop_var: bind_packages
17 +
18 + - name: Ensure Zone Directory is Created
19 +   file:
20 +     path: "{{ zone_dir }}"
21 +     state: directory
22 +     owner: root
23 +     group: root
24 +     mode: "0755"
25 +
26 + - name: Create Bind Conf File
27 +   template:
28 +     src: templates/named.conf
29 +     dest: "{{ bind_conf }}"
30 +     owner: root
31 +     group: "{{ bind_group }}"
32 +     mode: "0666"
```



Merge branch '249-rocky8' into 'master' Pin Straw authored 1 month ago

Jan 10, 2024

Adding Rocky 8 support: closes #249 Pin Straw authored 2 months ago

Nov 22, 2023

Merge branch 'issue-195' into 'master' Bryer Esengard authored 3 months ago

Nov 08, 2023

Merge branch into 'master' Pin Straw authored 4 months ago

regex Pin Straw authored 4 months ago

2024 CAE VM Automation

initial rocky9 template
Pin Straw authored 1 month ago 62da1fe8

Name	Last commit	Last update
📁 kali-template	Creating redteam kali template	2 months ago
📁 rocky9	initial rocky9 template	1 month ago
📄 .gitignore	Creating redteam kali template	2 months ago
📄 LICENSE	Adding LICENSE file	4 months ago
📄 README.md	Initial commit	4 months ago

```
PLAY RECAP *****
172.18.255.112      : ok=211  changed=80  unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.143      : ok=211  changed=80  unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.163      : ok=208  changed=75  unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.170      : ok=211  changed=80  unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.195      : ok=208  changed=75  unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.57       : ok=208  changed=75  unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.60       : ok=208  changed=75  unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.72       : ok=208  changed=75  unreachable=0    failed=0    skipped=10   rescued=0    ignored=0

Status changed to: successful
Ansible task is complete
Runner successful
[04:22:05] [default_event] provisioner )> █
```



CAE
IN CYBERSECURITY
COMMUNITY

2024 CAE

Further Insight

	Team0	Team1	Team2	Team3	Team4	Team5	Team6	Team7	Team8	Team9	Team10	Team11	Team12
SSH router rootteam	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
SSH router root_malicious_key	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
SSH router default_root	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
SSH shell rootteam	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
SSH shell mal_users	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
SSH shell ansible	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
SSH shell root_malicious_key	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
SSH shell default_root	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
SSH shell nobody	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
SSH www rootteam	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
SSH www mal_users	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
SSH www www-data	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH www ansible	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH www root_malicious_key	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH www default_root	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH www nobody	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH db rootteam	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH db mal_users	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
SSH db ansible	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH db root_malicious_key	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH db default_root	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH db nobody	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH dns rootteam	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH dns mal_users	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
SSH dns ansible	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH dns root_malicious_key	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH dns default_root	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
SSH dns nobody	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
Redis RCE Shell	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
Redis RCE DNS	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
Redis RCE WWW	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
Redis RCE MySQL	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛	⌛
Webmin DNS	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓
Webmin MySQL	↓	↓	↓	↓	↓	↓	↓	↑	↓	↓	↓	↓	↓



**NCAE
CYBERGAMES**
PLAY | LEARN | PROTECT

Symposium

2024 CAE

Importance?

Training: >

Students should be aware of the software and the modules that it has loaded. Modules that provide unnecessary or possibly malicious capabilities should be removed.

Justification: >

This challenge covers the skills required to analyze and evaluate the system's environment and identify suspicious additions to their system's configuration. The student must demonstrate that they determine a malicious module in legitimate software, and reconfigure the software to a functional and secure state.

Training: >

Students should be aware of how the package managers work on their system and where to look at the common configurations of them. By familiarizing themselves with different packages managers they will be able to move efficiently debug issues when trying to install packages.

Justification: >

This challenge covers the skills required to properly understand how the packages manager works across different Linux distributions and how to rectify any issues they may run into when trying to install software.



2024 CAE

Hacker Troll House



TROLLS DON'T PLAY FAIR

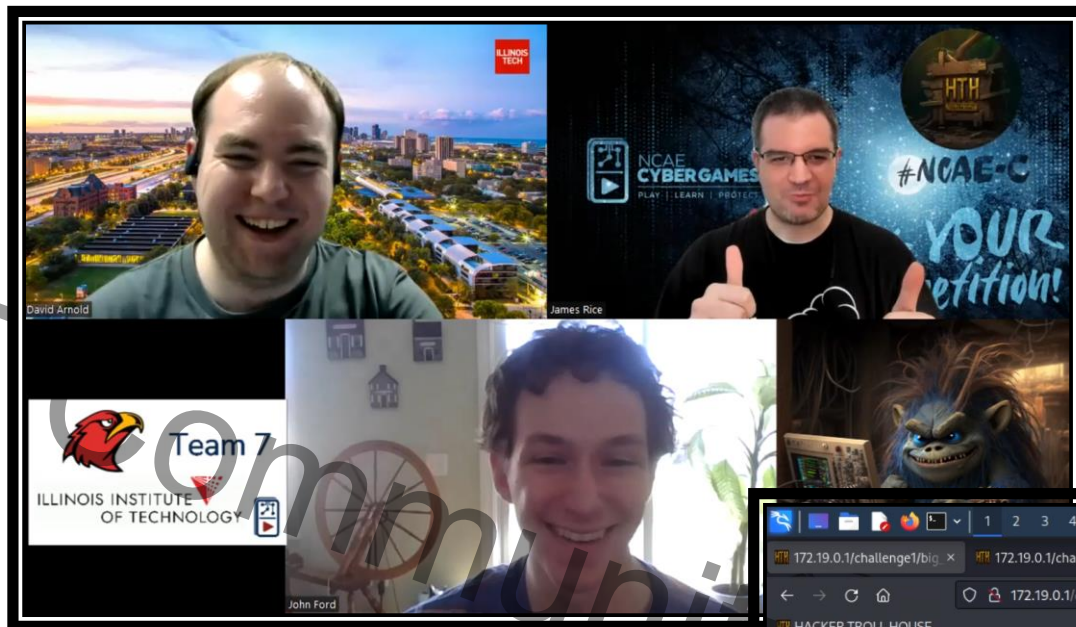
HIT H

HTSS THSIT THRTANI
TTSH H PINE HSTIGT

 Team 1 EMBRY-RIDDLE AERONAUTICAL UNIVERSITY DADE COLLEGE	 Team 2 EMBRY-RIDDLE AERONAUTICAL UNIVERSITY	 Team 3 UNIVERSITY OF WEST FLORIDA	 Team 4 LIBERTY UNIVERSITY	 Team 5 METRO STATE UNIVERSITY	 Team 6 EASTERN WASHINGTON UNIVERSITY	 Team 7 ILLINOIS INSTITUTE OF TECHNOLOGY	 Team 8 Tulsa	 Team 9 SYRACUSE S	 Team 10 BYU	 Team 11 Cal Poly Pomona	 Team 12 UF UNIVERSITY OF FLORIDA
---	---	---	---	--	--	---	---	---	--	---	--

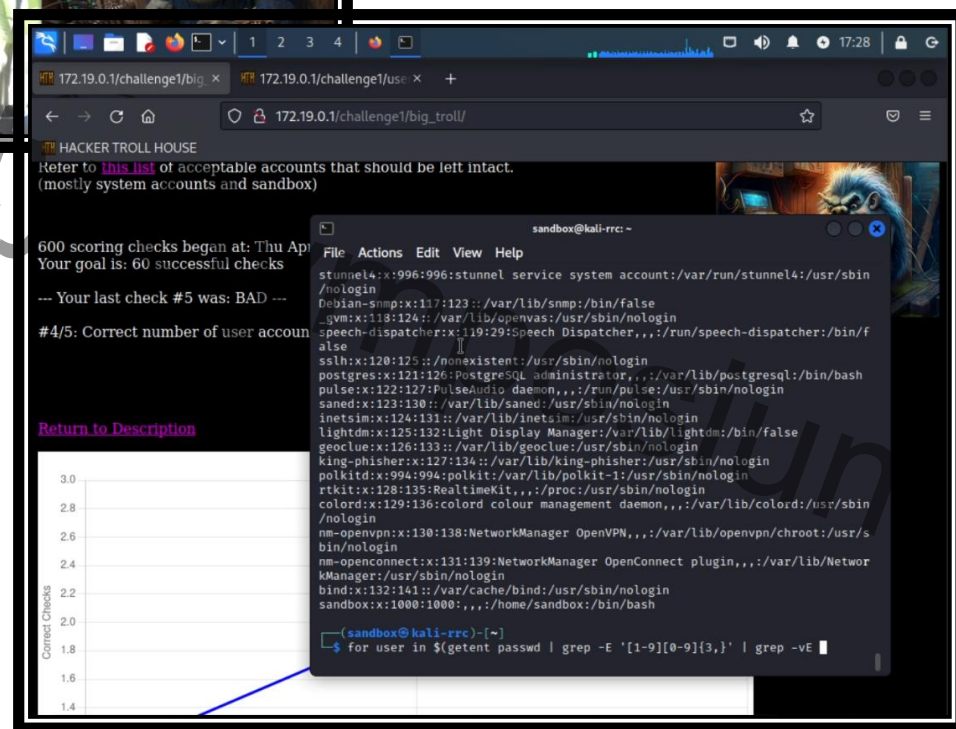
2023-2024 NCAE Cyber Games

CAE



Format: 2 students from each team selected for our in-person Invitational event.

Complete a series of fun challenges in a cyber gameshow style experience.



2024 CAE

Questions?

Swizzle

The
GALTHOUSE
LEGENDARY •  • LOUISVILLE

WALKER'S
Exchange



NCAE
CYBERGAMES

PLAY | LEARN | PROTECT